Remarks

Claims 1 to 19 are rejected.

Claims 1 to 3 and 5 to 19 remain in the application. Claims 1, 2, 5, 6, 8, 11 to 17 and 19 have been amended. Claim 4 has been withdrawn.

Specification

Please substitute the new paragraph 002 for old paragraph 002. Paragraph 002 has been amended to correct a typographical error.

Claim Rejections – 35 USC § 112

Claims 1, 2, 5, 6, 8, 11, 12, and 15 to 17 have been amended in order to avoid invoking 35 U.S.C. 112, sixth paragraph. In particular, all instances of phrases such as --the steps of-- have been deleted. Applicant wishes to note for the record that the amendments are neither narrowing, nor are the amendments being made for a reason substantially related to patentability. Applicant respectfully submits that no new matter has been added in the amendments.

Claim 19 has been rejected to under 35 USC § 112 as being indefinite due to inconsistent antecedence. Claim 19 has been amended and now recites, "predetermined criteria" instead of "the predetermined criteria", and thus now has consistent antecedence.

Claim Rejections – 35 USC § 102

Claim 1 has been rejected under 35 USC § 102 as being anticipated by US patent 4,720,860 (Weiss.) Claim 1 has been amended and now recites, "...providing at least a static parameter and at least a variable parameter selected from a plurality of variable parameters as a known password, the known password modifiable, as to the selected at least a variable parameter and as to a location and order of the at least a variable parameter within the known password..." In the system according to Weiss, the user provides a fixed secret code. The fixed secret code and variable input value are provided to as separate inputs of a function. The function provides a "non-predictable code" that is then provided by the user during authentication process. In the system of Weiss the "non-predictable code" is an output of a fixed function. The device of Weiss that receives the users fixed secret code and provides the non-predictable code is not described as being configurable and the function that it supports is not described as being suitable for modification once it is in regular use. Instead Weiss teaches that two separate devices provide equivalent non-predictable codes in order to authenticate a user. If the non-predictable codes do not match then the user is not authenticated. Applicant asserts that Weiss does not teach or suggest that any portion of the non-predictable result is or should be static. Given that a static value is inherently very predictable, Applicant questions the value of providing a "non-predictable" result in which some portion of the non-predictable result is static. Thus, it is asserted that a person of skill in the art, having reviewed and understood Weiss would not be lead to provide "at least a static parameter and at least a variable parameter selected from a plurality of variable parameters as a known password..." as recited in amended independent claim 1.

Therefore, it is clear that Weiss does not teach or suggest that the known password is "modifiable" as recited in amended independent claim 1. Therefore, amended independent claim 1 is no longer anticipated in light of Weiss. Similarly, it is apparent that amended independent claim 1 is not obvious in light of Weiss.

Claims 2, 3, and 5 have been rejected under 35 USC § 102 as being anticipated by Weiss. Claims 2, 3 and 5 depend from amended independent claim 1 which is not anticipated or obvious in light of Weiss. Therefore, claims 2, 3 and 5 cannot be either of anticipated or obvious in light of Weiss.

Claim 8 has been rejected under 35 USC § 102 as being anticipated by Weiss. The cited reference of Weiss teaches a system in which a same predetermined non-predictable function of time is executed on two separate devices. A first of those devices is disposed in data communication with an authentication server while the second device is provided to a user who wishes to be authenticated. When the user authenticates to the system the user provides a password based upon data provided by the second device. The authentication server receives this data and, in a comparison process compares data provided by the user to data provided by the first device.

Additionally claim 8 has been amended to more accurately describe who the "user" is. Specifically, claim 8 now recites:

> *"...wherein the known password is provided by a user and the static string is provided by the user."*

In the cited reference of Weiss the user provides the known password. If the user does not provide the known password then the user is not likely to be authenticated until they do. Additionally, Weiss does not suggest or mention that the user has any ability to change the password they provide. The variable password provided by the user is provided in direct response to the data presented to the user. Specifically, in the system suggested by Weiss, the password is defined such that the variable portion of the password is not subject to change based upon an accurate user input of a fixed code. Thus, the devices of Weiss that support the predetermined non-predictable code support the same code but are otherwise

independent. The device of Weiss receives user input data that is fixed and then informs the user what data is to be provided in order to be successfully authenticated. Reference Weiss, column 4, beginning line 18,

> *"In order to generate a code which will ultimately give the user clearance or access, the fixed code must be input into a predetermined algorithm which manipulates the fixed code as a static variable."*

Weiss simply does not suggest allowing the user to modify their password. Thus, Weis does not teach, "providing at least a static parameter and at least a variable parameter selected from a plurality of variable parameters as a known password" as recited in amended independent claim 1 from which amended claim 8 depends. As such, it is clear that amended claim 8 comprises a method that is not anticipated by Weiss. Additionally, Weiss does not teach or suggest that the user should be able to manipulate their password. Using the method of claim 8, a user is likely to choose a password that is quite complex, yet not so complex that they will fail to remember it. Conversely, the system according to Weiss is only secure to the extent that an unauthorized user is unable to obtain the fixed secret code (reference Weiss, column 4 lines 1 to 2) and a working device associated with that code. According to Weiss, once the fixed secret code is provided to the device, the device provides a non-predictable code. Referring to column 4, beginning on line 35,

> *"The non-predictable code 40 thus generated may be visually observed by the user for eventual input into an access control means 50,..."*

Thus, if an unauthorized user is able to accurately record a valid user authentication and then obtain the device of Weiss then that unauthorized user will be able to easily circumvent the security system of Weiss (Reference Column 5 lines 52 to 60 of Weiss.) In contrast, the method of claim 8 supports, "providing at least a static parameter and at least a variable parameter selected from a plurality of variable parameters as a known password,

the known password modifiable, as to the selected at least a variable parameter and as to a location and order of the at least a variable parameter within the known password;... wherein the known password is provided by a user and the static string is provided by the user." In this case, the user would not provide a consistent fixed code when authenticating. Clearly, a person of skill in the art will appreciate that ideally the user would provide a different data string each time that they authenticate and that the data string necessary for authentication would vary sufficiently quickly to prevent the use of the same data string at some later point in time. In which case, even if the user is accurately observed providing valid authentication static string data based upon their password, the variable nature of the password, according to amended claim 8 and amended independent claim 1, inhibits authentication using the same data string in the future. Conveniently, the method of claim 8 does not require that the user wishing to be authenticated have access to a separate device with them for authentication as suggested by Weiss. Therefore, it is apparent that amended claim 8 is not obvious in light of Weiss.

Claim 9 has been rejected as being anticipated by Weiss. Claim 9 recites:

> *"A method according to claim 8, wherein the known password is entered as a string of characters and wherein at least a character is indicative of one of a variable parameter and a static parameter."*

As described with reference to arguments regarding the anticipation rejection of claim 8 provided hereinabove, the known password of claim 9 clearly comprises a variable parameter. Weiss teaches a user providing a fixed access code (reference Weiss, column 4 lines 1 to 2) which is clearly different from the teaching of claim 9. Additionally, claim 9 depends from amended claim 8 and as amended claim 8 is neither anticipated nor obvious in light of Weiss, claim 9 cannot be either anticipated or obvious in light of Weiss.

Claim 10 has been rejected as being anticipated by Weiss. Claim 10 states:

> *"A method according to claim 9, wherein the string of characters is parsable to form the known password, the parsing distinguishing variable parameters from static parameters within the known password.*

In the office action, Examiner suggests that column 6, lines 16-33 of Weiss describes a string of characters that is parsable to form the known password. Applicant does not agree. Specifically, in the cited passage (ref. column 6, lines 16-33 of Weiss) it is clear that Weiss combines separate input signals comprising at least a variable parameter and fixed secret code data in a function to provide a non-predictable result. A person of skill in the art will appreciate that it is highly unlikely that the non-predictable result could be parsed into static parameters and dynamic parameters. As such, Weiss clearly does not teach that "the string of characters is parsable to form the known password, the parsing distinguishing variable parameters from static parameters within the known password" as recited in claim 10. Therefore, the cited reference of Weiss does not anticipate the claim 10 nor does it render claim 10 obvious. Further claim 10 depends from amended claim 8 and original claim 9, which are neither anticipated nor obvious in light of Weiss and, therefore, claim 10 cannot be either anticipated or obvious.

Claim 11 has been rejected as being anticipated by Weiss. Claim 11 has been corrected for an error in antecedence. Specifically claim 11 now states "the string of characters" instead of "the known password." Additionally, the notion of changing a password has been further clarified to ensure that it is understood that a user is changing the password. Further, the changing of a password is now recited outside of the preamble of the claim. Independent claim 11 now states:

> "A method comprising:
> changing a password of a user by:
> providing, from the user, a string of characters, the string including indications of at least a parameter from a plurality of parameters, the at least a parameter being a

variable parameter variable upon predetermined criteria;

receiving the provided string of characters; and,

storing data based on the string of characters in non-volatile memory, the data sufficient for verifying provided passwords to determine their accuracy."

Based upon the rejection stated by Examiner it is believed that Examiner is confused with regards to the method of claim 11. In Weiss, there is no mention of a format that the password will take, instead it is simply specified that a device generates a password based on data corresponding to a user input signal associated with a fixed secret code (ref. Weiss, col. 4, lines 1 and 2) and at least a dynamic variable provided internally by the device. A person of skill in the art will appreciate that somewhere in the device according to Weiss there are a set of memory locations that receive the user input signal and another set of memory locations that receive dynamic variable data. While Weiss does suggest that different numbers and types of dynamic variable generation are optionally supported Weiss does not suggest that a given device support configurable variable codes. Therefore, a person of skill in the art would appreciate that according to the cited reference of Weiss, it would be pointless to define a string of characters that describe a configuration for a valid password simply because only one configuration is supported and that configuration is fixed. Thus, it is clear that amended claim 11 is neither anticipated nor obvious in light of Weiss.

Claim 12 has been rejected as being anticipated by Weiss.

Examiner has stated, "Weiss discloses the step of extracting and storing static and dynamic data from the at least a variable parameter (col. 6, lines 16-21)." In the system of Weiss, a user provides data according to a fixed secret code to a device. The device generates dynamic data. The data according to the fixed secret code and the dynamic data are provided as inputs to a function that produces a "non-predictable" result. The word "parse" means (in the context of computing) analyze or separate into components. (Reference "parse" at www.dictionary.com) Thus, as this data is provided via separate

input signals in the system of Weiss it is apparent that parsing the data would be pointless because the fixed secret code and the dynamic data are provided from separate sources. Weiss uses both the data according to the fixed secret code and the dynamic data as separate and distinct input signals provided to a processor that processes a function that provides the non-predictable code. In contrast, the method of claim 12 relies on distinguishing variable parameters from static parameters within a known password. Such a step would be pointless in the device of Weiss. As Weiss does not teach or suggest, "...with a processor parsing the provided string of characters to distinguish static data from the at least a variable parameter", it is apparent that Weiss does not anticipate claim 12. Similarly, as a person of skill in the art having reviewed Weiss would not be lead to a system that incorporates "...parsing the provided string of characters to distinguish static data from the at least a variable parameter" it is apparent that the method of claim 12 is not obvious in light of Weiss. Additionally, claim 12 depends from amended claim 11, which is neither obvious nor anticipated. Therefore claim 12 cannot be either of anticipated or obvious.

Claim 15 has been rejected as being anticipated by Weiss. Claim 15 has been amended for consistency with the preamble of amended independent claim 11. Amended claim 15 clearly recites:

> ...extracting static data from the known password;
> hashing the extracted static data to determine at least a static hash value;
> storing the at least a static hash value; and,
> extracting dynamic data from the known password and storing indications of the dynamic data.

The cited reference of Weiss receives a fixed secret code from a user and data indicative of the current value of a dynamic variable. Since the inputs for this data are fundamentally separate it is apparent that no effort is required to separate them in a system and method of

Weiss. Thus, in the context of Weiss "extracting static data" is meaningless. The static data, which in the case of Weiss is the fixed secret code, is provided to the device independent of any other variable and, therefore, it does not need to be "extracted" from some other variable. With this in mind, it is apparent that Weiss does not anticipate claim 15. Additionally, as there is no use for "extracting static data from the known password" based upon the teaching of Weiss, it is apparent that a person of skill in the art would not be lead to doing so based upon Weiss. As such claim 15 is not obvious in light of Weiss. Further claim 15 depends from claim 11, which is neither anticipated nor obvious in light of Weiss and therefore claim 15 cannot be either of anticipated or obvious in light of Weiss.

Independent claim 16 has been rejected as being anticipated by Weiss. Claim 16 has been amended to remove the word "both" for clarity. Claim 16 clearly states:

> "...identifying static parameters within the string of characters;...
> comparing static parameters received within the string of characters with previously stored static parameters and the received dynamic parameter within the determined dynamic parameters to determine a first comparison result..."

In the cited reference of Weiss, this simply does not occur. Specifically, Weiss teaches having a user provide a fixed secret code to a device. The device generates data based upon a dynamic variable and then combines the data based upon the dynamic variable with the fixed secret code to provide a "non-predictable code". Weiss then compares non-predictable codes to authorize a user. Clearly, the non-predictable code is not a static parameter. Therefore, Weiss does not teach or suggest comparing static parameters as recited in claim 16. Thus, Weiss does not anticipate claim 16. Similarly, Weiss does not suggest "identifying static parameters within the string of characters" as recited in claim 16. In contrast, a system according to Weiss keeps static and dynamic data separate. In Weiss the static data is provided via a known interface that is only used for providing static data. Therefore, in the cited reference of Weiss there is no benefit to identifying static parameters. Once again, Weiss simply does not anticipate claim 16. Weiss does not use

static parameters for anything other than input data for a non-predictable function. Therefore, a person of skill in the art having reviewed and understood Weiss would not be lead to the invention of claim 16.

Claim 17 has been rejected as being anticipated by Weiss. Claim 17 has been amended to ensure consistency with regards to the variable parameters. In the cited reference of Weiss, a user provides a fixed secret code to a device. The device receives a data based on an internally generated dynamic variable as well as the fixed secret code. These two data values are then used as inputs provided to a function that outputs a "non-predictable" result. This result is then used to authenticate the user. The method of claim 17 states:

> "A method of generating a dynamic password comprising:
> providing a process for transforming at least a variable parameter into an ordered string of characters, wherein the process sometimes results in different ordered strings of characters for a same variable parameter; and,
> providing the at least a variable parameter as a password, the provided variable parameter provided by an individual via a data entry device.

A difference between the method of the cited reference of Weiss and the method of independent claim 17 is that in Weiss the static string of characters would be provided as a password. In contrast, the method of independent claim 17 uses "at least a variable parameter" as a password that is "provided by an individual via a data entry device". This difference is very important to the method of independent claim 17. Specifically, in Weiss, the device itself provides a dynamic data portion internally. Clearly, this is inconsistent with independent claim 17 and, therefore, independent claim 17 is not anticipated by Weiss. Similarly, Weiss does not render claim 17 obvious.

Claims 18 and 19 depend from independent claim 17. As independent claim 17 is neither

anticipated nor obvious neither of claim 18 and 19 are anticipated or obvious.

Claim Rejections – 35 USC § 103

Claims 6 and 7 have been rejected as being obvious in light of the combination of Weiss and US patent 6,209,104 (Jalili). independent claim 6.

Claim 6 states:

> "... wherein the process includes providing data to a user for interpretation by the user and then comparing the user's interpretation to a predetermined known interpretation."

Claim 6 depends from amended independent claim 1. As amended independent claim 1is not obvious in light Weiss it is apparent that dependent claim 6 cannot be obvious in light of Weiss. Further, the cited reference of Weiss teaches a system in which a user provides a static string to a computing device. The computing device uses data from the static string in addition to a variable code produced internally by the computing device as inputs to a function. This function provides a "non-predictable code" as an output. This code is provided on a display that a user provides as an authentication signal to a system. Weiss does not teach "providing data to a user for interpretation by the user" nor does Weiss teach "comparing the user's interpretation to a predetermined known interpretation." Therefore amended independent claim 6 is not obvious in light of Weiss in isolation.

The cited reference of Jalili teaches substituting an icon for a value to make it harder for an observer to learn a static code. The user provides an input signal in which a value is based on a number of petals on a flower icon or a number of bowling pins in a bowling pin icon etc. The icons are provided in pseudo randomly placed locations on a screen. A user inputs data according to their static, secret code by selecting icons. The locations of the icons selected are provided as a user input signal that is a "static string". This static string is then interpreted to provide the password. Jalili does not teach,

"providing a process for transforming at least a variable parameter into an ordered string of characters, wherein the process sometimes results in different ordered strings of characters for a same variable parameter;
providing at least a static parameter and at least a variable parameter selected from a plurality of variable parameters as a known password, the known password modifiable, as to the selected at least a variable parameter and as to a location and order of the at least a variable parameter within the known password..."

Applicant is of the opinion that Jahili is teaching providing a static password based upon a fixed interpretation of a variable parameter. This interpretation of a variable parameter is then used by a computing device to generate the static password. This is not equivalent to "providing at least a static parameter and at least a variable parameter selected from a plurality of variable parameters as a known password" as recited in amended independent claim 1. As such, it is apparent that amended independent claim 1 is not obvious in light of Jahlili in isolation, and therefore claim 6 cannot be obvious in light Jahlili in isolation.

Applicant asserts that a person of skill in the art of encryption would not be lead to a method according to the invention upon reviewing and understanding the cited references of Weiss and Jahlili. Specifically, Weiss acknowledges that the system of Weiss can be made to provide valid codes if:

a) An unauthorised user is able to observe the entry of a static code in the system of Weiss and,

b) The unauthorized user has access to working device of Weiss.

Jahlili focuses on ensuring that static data provided to device is provided in a way to complicate accurate observation of the data. Therefore, a person of skill in the art would be lead to combine these references by using the teaching of Jahlili to increase the difficulty of observing the entry of the static code in the system of Weiss. Such a method is quite different from the method described by amended independent claim 6. Therefore, it is apparent that amended independent claim 6 is not obvious in light of Weiss in

combination with Jahlili.

Applicant asserts that there is no common teaching in Weiss and Jahlili that would lead a person of ordinary skill in the art to combine them in a way to produce a method consistent with the method of claim 6. Specifically, neither Weiss nor Jahlili teach, "providing data to a user for interpretation by the user and then comparing the user's interpretation to a predetermined known interpretation" as recited in amended independent claim 6. Clearly, Weiss simply provides an alpha numeric string to a user that the user then provides for their authentication. Jahlili provides data to user but the data is provided in a way that does not take a user's interpretation of it into account. Specifically, in Jahlili, an icon representing three bowling pins is automatically assigned a value of "3". If the user were to provide their interpretation of three bowling pins then the user might provide a different response. For example, a first user might chose interpret the bowling pin icon as described by Jahlili (Jahlili Fig. 5 and associated description col. 7 lines 15 to 23.) A second user might attribute a different value to the same icon. For example, the second user could interpret the value of the icon as follows: take the number of items displayed in the icon and add a value based on the position in the alphabet of the first letter of an adjective that describes the item shown, where "A"='a'= 0, "B"="b"=1, "C"="c"=2... Thus, the second user sees three bowling pins and interprets the icon to be a "4" (3 + 1, where the 1 is indicative of "b" for the adjective "bowling".) Using the method of claim 6, different users could have different interpretations of an image. This interpretation severely complicates reproduction of the user's password by observation. Clearly, such an arrangement is not contemplated by Jahlili nor Weiss however it is supported by claim 6 and amended independent claim 1 from which it depends. Specifically, if a user in authenticating with a system according to Jahlili provides their own interpretation of an icon in which their interpretation differs from the fixed interpretation of the system then it is unlikely that the user will be authenticated. It is clear that supporting different user's interpretations of data complicates the circumventing of an authorization process. With this in mind it is apparent

that claim 6 provides advantages over the cited references of Weiss and Jahlili that are not suggested by either reference in isolation and would not be apparent to one of ordinary skill in the art having reviewed those cited references. For these reasons, it is apparent that claim 6 is not obvious in light of the combination of Weiss and Jahlili.

Claim 7 recites, "the provided data is an image and the interpretation is a string indicative of the image." Arguments provided with respect to obviousness of claim 6 in light of Weiss in combination with Jahlili are equally applicable for claim 7.

Examiner has rejected claim 13 as being obvious in light of the combination of Weiss and US patent 6,209,104 (Jalili). Claim 13 has been amended. Specifically, the word "variable" has been inserted prior to the first instance of the word "parameters" for enhanced clarity.

Applicant asserts that the cited reference of Weiss does not describe or suggest the limitation "wherein the variable parameters are selected from a plurality of available parameters and wherein the plurality of available parameters are provided to the user for selecting thereform." Specifically, Weiss teaches providing a "fixed secret code" to a device and receives dynamic inputs. Data relating to the fixed secret code and the dynamic inputs are then used to provide a non-predictable code. The fixed secret code obviously does not correspond to a variable parameter. The dynamic inputs are provided to the device internally in the teaching of Weiss and therefore it would be reasonable to describe them as being variable parameters. That said, Weiss does not teach a system that allows a user to select the variable parameters used to authenticate them. In contrast, the method of amended claim 13 teaches:

> *"providing a string of characters, the string including indications of at least a parameter from a plurality of parameters, the at least a parameter being a variable*

parameter variable upon predetermined criteria...wherein the plurality of available parameters are provided to the user for selecting thereform."

Thus, the method of amended claim 13 supports the user selecting from a plurality of available parameters and the plurality of available parameters comprises a variable parameter. Weiss does not teach or suggest this and therefore the method of amended claim 13 is not obvious in light of Weiss in isolation.

The cited reference of Jalili teaches an authentication system in which a set of icons indicative of values are provided for selection by a user. Jalili does not specify that the user is able to choose the parameters associated with their authentication. Instead, Jalili provides a user with an image comprising symbolic representations of, for example, numbers. The user then provides an input signal corresponding to an ordered series of numbers. Effectively, Jalili is disguising numbers but in the cited reference of Jalili the user is still responsible for providing a specific number, such as a credit card number, in order to authenticate. Claim 13 recites,

"storing data based on the string of characters, the data sufficient for verifying passwords provided by a user to determine their accuracy, wherein the variable parameters are selected from a plurality of available parameters and wherein the plurality of available parameters are provided to the user for selecting thereform."

Claim 13 supports the user selecting from a plurality of available parameters. Jalili simply does not teach this. Instead, in the cited reference of Jalili the parameter, for example a type of icon representing a number, is chosen for the user, the user then selects icons corresponding to a number that they use to authenticate with. If the user does not choose the icons corresponding to the number that they authenticate with then the user is likely not to be authenticated. Therefore, claim 13 is not obvious in light of Jalili in isolation.

A person of skill in the art of encryption having read and understood both Jalili and Weiss would not be lead to the method of claim 13. Neither Jalili nor Weiss teach,

"providing a string of characters, the string including indications of at least a parameter from a plurality of parameters, the at least a parameter being a variable parameter variable upon predetermined criteria...wherein the plurality of available parameters are provided to the user for selecting thereform."

In both Jalili and Weiss, the user is provided an interface and must provide a specific code to be authenticated. The user is unable to select variable parameters associated with that specific code in either of Jalili or Weiss. Therefore amended claim 13 is not obvious in light of the combination of Jalili and Weiss.

Further having carefully reviewed the cited references of Weiss and Jalili, Applicant is of the opinion that a person of skill in the art tasked with providing a highly secure authentication system having reviewed the cited references would provide a device substantially different from the devices described in claims 13 and 14. Specifically, Weiss teaches a system in which a user provides a fixed secret code to a device that receives the fixed secret code data and data associated with a dynamic variable. The two sets of data are used as inputs to a function that provides a non-predictable result. This result is then used for authentication. In contrast, Jalili uses icons to represent variables thereby inhibiting an observer from observing the providing of a fixed input used for authentication. Combining these references would lead one of skill in the art to provide a device that provides an interface in which a user selects a set of icons in specific order according to a fixed secret code. The icons are associated with specific values and the device provides the value as an input to a function. The function receives the fixed secret code along with data from a dynamic variable, as clearly described by Weiss, to provide a non-predictable code. The non-predictable code is then used to authenticate the user. Since the non-predictable code generated by the device is only temporarily useable that code would likely not be input by selecting a series of icons as taught by Jalili.

Claim 14 depends from amended claims 11 and 13. As amended claims 11 and 13 are not

obvious it is apparent that claim 14 cannot be obvious.

No new matter has been added.

A Petition for Extension of Time is filed concurrently with this response.

Please charge any additional fees required or credit any overpayment to Deposit Account No. 50-1142.

Applicant requests favourable reconsideration of the amended application.

Respectfully submitted,

Gordon Freedman, Reg. No. 41,553

Freedman and Associates
117 Centrepointe Drive, Suite 350
Nepean, Ontario
K2G 5X3 Canada

Tel (613) 274-7272
Fax (613) 274-7414

VL/sah